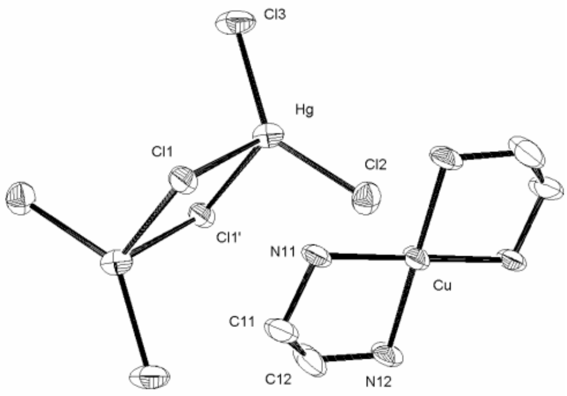
scip ag

Contents

1. Editorial

MySkypeWorm - Connecting with Friends

Das Internet habe ich seit jeher als Kommunikations- und Informationsmedium betrachtet. Unzählige Stunden habe ich in Chats verbracht und mit Leuten im Usenet sowie in Webforen diskutiert.



Mit multimedialen Kommunikationslösungen wie Skype haben aber viele die Nützlichkeit des Netzes für sich entdeckt, die zuvor dem Ganzen sehr skeptisch gegenübergestanden sind. Auch ich selbst bin einer der ersten Skype-Benutzer gewesen. Obschon ich sagen muss, dass die schlechte technische Implementierung und das strenge closed-source Prinzip (zudem viele Obfuscation-Mechanismen im Binary) mir gänzlich widerspricht, vermag die Ergonomie und Einfachheit der Software zu überzeugen. Zu Recht wird Skype als beliebteste Lösung seines Bereichs verstanden.

Als ich mich mit etwa 12 Jahren intensiver mit Computerviren und -würmern auseinanderzusetzen begann, war das Internet für mich damals noch in weiter Ferne. Mit dem Zugang zum Netz der Netze wurde jedoch auch mein Verständnis für sich selber reproduzierenden Programmcode gänzlich auf den Kopf gestellt: Viren sollten nicht mehr nur per Disketten (Dateiviren und Bootsektorviren) übertragen werden, sondern konnten sich als autonome Würmer durch vernetzte Umgebungen bewegen.

Mein Interesse an solcher Software habe ich nie verloren, wenn ich mich auch zwischenzeitlich eher für andere Aspekte der Informationssicherheit zu interessieren begann.

Dieses Wochenende verbrachte ich damit an meinem neuen Buch zu schreiben. Es ging ein bisschen harzig voran, denn irgendwie waren die Gedanken noch nicht so sortiert, wie ich das gern gehabt hätte. Doch dies ist die elementare Voraussetzung für ein gutes Schriftstück. Gut Ding will Weile haben und so entschied ich mich, um mein Gehirn ein bisschen zu durchlüften, etwas anderes zu tun.

Da ich vor Kurzem den Nutzen von Skype wieder für mich entdeckt hatte, und mich schon immer die API des Clients interessierte, wollte ich mal eben schnell einen Skype-Wurm schreiben (und schliesslich ist in den News-Portalen die Rede eines neuen Orkut-Wurms namens W32.Scrapkut). Die Idee eines solchen Schädlings war nicht neu, wurde denn Ende Dezember 2006 erstmals eine echte Implementierung in-the-wild gesichtet.

Die erste Umsetzung eines Skype-Wurms nutzte das Prinzip, welches am einfachsten schien: Der Schädling öffnete einen Chat mit einer Person in der Kontaktliste und schickte über diesen einen Download-Link zu einer Kopie von sich selbst. Eigentlich ist dies kein echter Wurm, denn er reproduziert sich nicht über das gleiche Medium. Viel mehr ist der Skype-Trojaner quasi ein Advertising-Element für sich selbst. Der Benutzer muss noch immer über einen Webbrowser die korrupte EXE-Datei vom Webserver herunterladen und ausführen, um das

Advertising weiterzuführen. Früher nannte man soetwas auch scherzhaft Signatur-Virus. Dem konnte nun relativ einfach entgegengewirkt werden, indem (1) die korrupten EXE-Dateien von den Webservern gelöscht, (2) der Zugriff auf die bösartigen URLs unterbunden und (3) Skype-Nachrichten mit derartigen Links gefiltert wurden.

Meine Implementierung sollte raffinierter ausfallen (andere Ansätze wurden ja rund ein Jahr später schon verfolgt). Zum einen wollte ich effektiv, dass sich der Wurm über Skype selber repliziert und nicht auf externe Quellen angewiesen ist. Mein Wurm sollte also einen internen File-Transfer initiieren. Das Problem ist, dass mit dem API-Call "OPEN FILETRANSFER" zwar ein solcher angegangen werden kann. Als erster Parameter wird dabei der Benutzername des Empfängers angegeben. Als zweiten Parameter lässt sich jedoch lediglich das Verzeichnis definieren, welches in der Auswahl geöffnet werden will. Eine direkte Angabe eines Pfads inklusive Dateinamens ist nicht möglich und generiert die allgemeine Fehlermeldung "ERROR 109 OPEN directory doesn't exist".

Ich behalf mich eines unpopulären Tricks. Sodann öffne ich das Verzeichnis, in dem sich die Kopie meines Skype-Wurms befindet im Transfer-Fenster. Durch das senden von Koordinaten an die Maus und Klickanweisungen an selbige kann ich sodann die Datei über die GUI-Steuerung auswählen lassen. Dies geschieht innert Millisekunden und ist durch den Benutzer weder grossartig einsehbar noch überhaupt verhinderbar. Den gleichen Effekt pflege ich bei meiner Cracking-Software PGPSDACrack zu verwenden, mit der passwortgeschützte PGP-EXE-Archive angegriffen werden können. Der Benutzer muss nur noch den Datentransfer akzeptieren und danach die EXE-Datei ausführen. Um diesen Prozess zu optimieren, wird zuvor ein Chat mittels "CHAT CREATE" gestartet und über "CHATMESSAGE" eine manipulative Social Engineering-Nachricht verschickt. In dieser wird der Empfänger des Dateitransfers darauf hingewiesen, dass es sich hier um einen speziellen Patch für Skype handelt, durch den der Client um wichtige und interessante Funktionalitäten erweitert werden kann. Das Thema kann natürlich beliebig angepasst werden.

Das Problem solcher Nachrichten, die bei modernen Mailwürmern ebenso eine wichtige Rollen spielen, ist die Lokalisation. Es erscheint unsinnig, dass ich zum Beispiel meiner Mutter ein Email auf Englisch schreibe und darin um das Ausführen einer angehängten EXE-Datei (dem Virus) bitte. Mit ihr würde ich definitiv auf Deutsch kommunizieren, so dass die falsche Sprachwahl sofort auffallen würde. Mein Wurm liest sodann aus dem Skype-Profil des Enpfängers dessen Herkunft aus und richtet sich damit in der Sprachwahl nach den lokalen Bedingungen. Die über die Chat-Kommunikation mitgeteilten Phrasen müssen also nur noch übersetzt werden, so dass der Verdachtsmoment auf ein Minimum reduziert werden kann.

Ist ein System einmal mit dem Skype-Wurm infiziert, überwacht dieser ständig den Status des Skype-Clients. Ist dieser verbunden und sind irgendwelche Kontakte online, werden ihnen in mehr oder weniger zufälliger Reihenfolge (siehe auch "SEARCH USERS") der Wurm über den eben genannten Weg zugeschickt. Dabei speichert der Wurm, welche Benutzer den Datentransfer schon durchgeführt haben und welche nicht. Damit soll eine mehrmalige Infektion verhindert sowie der wiederholte Infektionsversuch unterbunden werden. Der Skype-Wurm überwacht ebenfalls, ob er Ziel eines Infektionsversuchs ist. Ist dies der Fall, wird der Datentransfer sofort abgebrochen. Der Infector weiss sodann ebenfalls, dass das Zielobjekt schon erfolgreich angegangen wurde und sieht damit von einer weiteren Übertragung ab.

Mein Ansatz hat zwei entscheidende Vorteile. (1) Zum einen ist man bei der Bereitstellung des korrupten Programmcodes nicht mehr auf andere Medien, im zuvor genannten Fall auf einen Webserver, angewiesen. Der Wurm propagiert und verbreitet sich autonomisch über Skype. (2) Dies führt zeitgleich dazu, dass solange mindestens ein infizierter Client im Internet ist, der Wurm theoretisch noch immer dezentral agieren kann. Es kann nicht mehr nur einfach ein zentraler Webserver deaktiviert werden, um die Wurmverbreitung zu unterbinden. Zudem weisen die von mir eingebrachten Mechanismen eine zusätzliche Polymorphie auf, sind sie ohne tiefschürfende Eingriffe in die API von Skype nahezu unmöglich zu bekämpfen.

Mit dieser kleinen Denkpause, die ich mir gegönnt habe, habe ich einmal mehr sehr viel über Instant Messaging, Skype, dessen API und die Möglichkeiten moderner Computerwürmer gelernt. Die Hürde des automatischen Dateitransfers ist kleiner, als man dies hätte annehmen könnte. Und so wird es nur eine Frage der Zeit sein, bis jemand anderes auf die gleiche Idee kommt wie ich. Mein kleiner Skype-Wurm bleibt jedenfalls bei mir, schön verschlossen in meinem Development-Folder. Wäre ich so töricht und würde ihn freilassen, würde ich mir wohl kaum Freunde machen. Doch das ist es ja eigentlich das, was man mit Facebook, MySpace, StudiVZ und Xing machen möchte. Vielleicht sollte ich mir mal die Möglichkeiten der Sozialen Netzwerke mit ihren eigenen Nachrichten-systemen genauer anschauen... Doch das spar ich mir für die nächste Pause.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 2. März 2008

2. scip AG Informationen

2.1 Telnetrecon

Das als integrales Fingerprinting-Framework angelegte Projekt von Marc Ruef welches im scip monthly Security Summary vom 19. Dezember 2007 mit der Publizierung des httprecon Projekts (http://www.computec.ch/projekte/httprecon/) begann wird in Kürze einen weiteren Ableger erhalten. Es handelt sich dabei um das telnetrecon project.

http://www.computec.ch/projekte/telnetrecon/

Das telnetrecon project erforscht dabei das Gebiet des Telnet Server Fingerprinting. Das Ziel des Projektes ist die akkurate Identifikation der gegebenen Implementation des entsprechenden Telnet Servers.

2.2 Computerworld

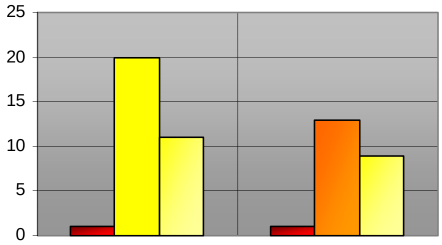
Marc Ruef beantwortete in der am 5. März 2008 erschienenen Ausgabe der Computerworld (http://www.computerworld.ch) wie man mittels Security Audits bzw. Backdoor Inside/Out Attacken testen kann, wo die IT-Security wirklich steht insbesondere der Schutz gegen Computerviren.

http://www.computerworld.ch/aktuell/itsecurity/44095/

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter http://www.scip.ch/cgi-bin/smss/showadvf.pl einsehbar.

Die Dienstleistungspakete)scip(pallas liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.



	Feb 08	Mrz 08
sehr kritisch	1	1
kritisch	20	13
problematisch	11	9

Contents:

3.1 VMware Server authd Pufferüberlauf

Einstufung: problematisch
Remote: Ja
Datum: 17.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3652

VMware, Inc., ist ein US-amerikanisches Unternehmen, das Software im Bereich der Virtualisierung herstellt. Die Firma wurde 1998 mit dem Ziel gegründet, eine Technik zu entwickeln, virtuelle Maschinen auf Standard–Computern zur Anwendung zu bringen. Das bekannteste Produkt ist VMware Workstation. In seinen Updates Notes beschreibt VMware eine Schwachstelle im VMware Server, bei dem durch einen unspezifizierten Pufferüberlauf in authd beliebiger Code zur Ausführung gebracht werden kann.

Expertenmeinung:
VMware ist ein populäres Produkt geworden. Mit der immer günstiger werdenden Hardware ist eine derartige Virtualisierungsinfrastruktur heute relativ einfach aufzubauen. In einer neuen Version von VMWare Server werden verschiedene Probleme adressiert, die in den Vorgängerversion präsent sind. Administratoren sollten dieses Update berücksichtigen, um das Risiko eines erfolgreichen Angriffs zu minimieren.

3.2 Nagios unspezifiziertes Cross-Site Scripting

Einstufung: problematisch
Remote: Ja
Datum: 14.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3651

Durch die Software Nagios (Network + Hagios), die früher NetSaint hiess, ist es möglich, komplexe IT-Strukturen zu überwachen. Nagios bietet dazu eine Sammlung von Modulen zur Netzwerk-, Host- und speziell Serviceüberwachung sowie einem Webinterface zum Abfragen der gesammelten Daten. Nagios steht unter der GPL, ist also Freie Software, und läuft unter zahlreichen Unix-ähnlichen Betriebssystemen. Nagios und das Nagios-Logo sind eingetragene Warenzeichen von Ethan Galstad. Der Hersteller selber berichtet in einem Advisory von einer Schwachstelle, die dadurch entsteht dass gewisse unspezifizierte Eingaben nur unzureichend validiert werden, was die Ausführung webbasierter Angriffsmethoden erlaubt.

Expertenmeinung:
Mit dem stets wachsenden Erfahrungsschatz im Bereich des Web Exploitings werden solche Schwachstellen zunehmend gefährlicher, als sie es so oder so schon sind. Das Problem der Script Injection wird in diesem Kontext nach wie vor zu wenig ernst genommen. Im vorliegenden Fall empfiehlt sich die Einspielung des freigegebenen Patches binnen nützlicher Frist.

3.3 Internet Explorer FTP Command Injection

Einstufung: problematisch
Remote: Ja
Datum: 12.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3650

Windows Internet Explorer (früher Microsoft Internet Explorer, Abkürzung: IE oder auch MSIE) bezeichnet einen Webbrowser von Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95b, SR2 ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei älteren Windows-Versionen kann er nachinstalliert werden. Den „Microsoft Internet Explorer“ gab es für einige Zeit auch Versionen für Mac OS und Unix-Derivate (wie Solaris und HP-UX). Die derzeit aktuelle Version ist Windows Internet Explorer 7. Derek Abdine fand in den Versionen bis und mit 6.x eine Schwachstelle, bei der sich beliebige FTP Befehle mittels speziell vorpräparierter URIs injizieren lassen. Dadurch kann unter Umständen erreicht werden, dass Schadcode von einem entfernten Server heruntergeladen und unter Umständen ausgeführt wird.

Expertenmeinung:
Eine Lösung für dieses Problem hat Microsoft bislang offenbar nicht gefunden, weshalb derzeit darauf verwiesen wird, auf Internet Explorer 7 umzusteigen - was natürlich ebenfalls im Interesse des Softwaregiganten sein dürfte. Viele Administratoren dürften für diese Variante allerdings wenig Begeisterung aufbringen. In diesem Fall gilt es, bewusst mit dem hier illustrierten Risiko umzugehen und einen allfällig noch erscheinenden Patch zeitnah einzuspielen.

3.4 Microsoft Office unspezifizierter Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 11.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3649

Microsoft Office ist das Office-Paket der Firma Microsoft für Microsoft Windows und Mac OS. Für unterschiedliche Aufgabenstellungen werden verschiedene Suiten angeboten, die sich in den enthaltenen Komponenten und im Preis unterscheiden. Microsoft publizierte unlängst eine Schwachstelle in verschiedenene Office Versionen, bei denen sich durch einen unspezifizierten Fehler in einer Office Komponente ein Pufferüberlauf provozieren und beliebiger Code zur Ausführung bringen lässt.

Expertenmeinung:
Grosszügig mit Informationen ist Microsoft im Bezug auf die vorliegenden Schwachstellen nicht gerade, was die Einschätzung erschwert. Es sei daher schlicht angeraten, die freigegebenen Patches zeitnah zu installieren um eine Ausnutzung zu vermeiden.

3.5 Microsoft Office Excel-File Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 11.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3648

Microsoft Office ist das Office-Paket der Firma Microsoft für Microsoft Windows und Mac OS. Für unterschiedliche Aufgabenstellungen werden verschiedene Suiten angeboten, die sich in den enthaltenen Komponenten und im Preis unterscheiden. Microsoft publizierte unlängst eine Schwachstelle in verschiedenene Office Versionen, bei denen sich durch einen unspezifizierten Fehler in Excel ein Pufferüberlauf provozieren und beliebiger Code zur Ausführung bringen lässt.

Expertenmeinung:
Grosszügig mit Informationen ist Microsoft im Bezug auf die vorliegenden Schwachstellen nicht gerade, was die Einschätzung erschwert. Es sei daher schlicht angeraten, die freigegebenen Patches zeitnah zu installieren um eine Ausnutzung zu vermeiden.

3.6 Microsoft Outlook "mailto:" URI Handling Vulnerability

Einstufung: sehr kritisch
Remote: Ja
Datum: 11.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3647

Outlook (OL) (für Windows) und Entourage (für Mac OS) sind verbreitete Personal Information

Manager der Firma Microsoft. Die Windows-Version heißt Outlook, die Macintosh-Version dagegen seit 2001 Entourage. Vom Funktionsumfang her sind beide Produkte ähnlich. In Outlook fand Greg MacManus von iDefense eine Schwachstelle bei der Verarbeitung speziell manipulierter mailto: URIs, die von einem Webbrowser übergeben werden. Durch diese können zusätzliche Kommandozeilenargumente an Outlook übergeben werden. Basierend darauf kann beliebiger Code ausgeführt werden, wenn ein Benutzer eine präparierte Webseite besucht.

Expertenmeinung:
Outlook, so muss man sagen, besitzt schon seit Jahren nicht unbedingt den Ruf zu den sichersten Applikationen seiner Klasse zu gehören. Viele Unkenrufe der Vergangenheit waren sicherlich auch durch persönliche Präferenzen gegenüber dem Hersteller Microsoft bedingt, im vorliegenden Fall dürften sich alle Kritiker aber erneut im Recht sehen. Der Schwachstelle, die bereits aktiv ausgenutzt wird, sollte mittels dem baldmöglichsten Einspielen des freigegebenen Patches entgegengewirkt werden.

3.7 Check Point VPN-1 UTM Edge Cross-Site Scripting

Einstufung: problematisch
Remote: Ja
Datum: 06.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3646

Check Point Software Technologies Ltd. ist ein Softwareunternehmen bekannt mit ihren Firewall- und VPN-Produkten. Die Firma wurde 1993 in Ramat Gan, Israel gegründet und beschäftigt etwa 1800 Mitarbeiter. Der Hauptsitz ist in Redwood City in USA, Entwicklung und der internationale Hauptsitz in Ramat-Gan. Nach Angaben von Check Point nutzen alle der Top100 Unternehmen Sicherheitslösungen der Firma. Im Produkt Check Point VPN-1 UTM Edge existiert eine Schwachstelle, bei der durch die unzureichende Validierung des "user" Parameters auf der Loginseite der Lösung beliebige webbasierte Angriffsmöglichkeiten ausgeschöpft werden können.

Expertenmeinung:
Mit dem stets wachsenden Erfahrungsschatz im Bereich des Web Exploitings werden solche Schwachstellen zunehmend gefährlicher, als sie es so oder so schon sind. Das Problem der Script Injection wird in diesem Kontext nach wie vor zu wenig ernst genommen. Im vorliegenden Fall empfiehlt sich die Einspielung des freigegebenen Patches binnen nützlicher Frist.

3.8 Sun Java JDK / JRE Raw Socket Umgehungsangriff

Einstufung: kritisch
Remote: Ja
Datum: 05.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3644

Die Java-Plattform (englisch Java Platform) definiert die Ablaufumgebung (Java Virtual Machine) und Programmierschnittstellen (Java Application Programming Interface) innerhalb der Java-Technologie. Der Kern der Java-Plattform ist die Java-Laufzeitumgebung (englisch Java Runtime Environment). In verschiedenen Java Paketen wurde eine Schwachstelle identifiziert, durch die mittels eines unspezifzierten Fehlers im JRE beliebige Netzwerkverbindungen durch den Browser des Betroffenen durchgeführt werden können.

Expertenmeinung:
Als populäre Plattform bietet Java ein gerngesehenes Angriffsziel, das auch frequent eingehend untersucht zu werden scheint. Ganze elf Schwachstelle fixt Sun im neusten Update seiner verschiedenen Java-Distributionspakete. In ihrer Kritikalität sind sämtliche Schwachstellen als "kritisch" zu bewerten. Sun hat weiterhin zu einigen Schwachstellen keine Details veröffentlicht, was gemeinhin als tendentiell eher unheilvolles Zeichen zu deuten ist. Nachdem Kompatibilitätsüberprüfungen durchgeführt wurden, sollten Administratoren baldmöglichst die Einspielung aktualisierter Versionen anstreben um die Ausnutzung der hier aufgezeigten Schwachstellen zu vermeiden.

3.9 Sun Java JDK / JRE Java Web Start unspezifizierte Codeausführung

Einstufung: kritisch
Remote: Ja
Datum: 05.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3641

Die Java-Plattform (englisch Java Platform) definiert die Ablaufumgebung (Java Virtual Machine) und Programmierschnittstellen (Java Application Programming Interface) innerhalb der Java-Technologie. Der Kern der Java-Plattform ist die Java-Laufzeitumgebung (englisch Java Runtime Environment). In verschiedenen Java Paketen wurde eine Schwachstelle identifiziert, durch die mittels eines unspezifzierten Fehlers in Java Web Start beliebiger Code zur Ausführung gebracht werden kann.

Expertenmeinung:
Als populäre Plattform bietet Java ein gerngesehenes Angriffsziel, das auch frequent eingehend untersucht zu werden scheint. Ganze elf Schwachstelle fixt Sun im neusten Update seiner verschiedenen Java-Distributionspakete. In ihrer Kritikalität sind sämtliche Schwachstellen als "kritisch" zu bewerten. Sun hat weiterhin zu einigen Schwachstellen keine Details veröffentlicht, was gemeinhin als tendentiell eher unheilvolles Zeichen zu deuten ist. Nachdem Kompatibilitätsüberprüfungen durchgeführt wurden, sollten Administratoren baldmöglichst die Einspielung aktualisierter Versionen anstreben um die Ausnutzung der hier aufgezeigten Schwachstellen zu vermeiden.

3.10 Sun Java JDK / JRE Java Web Start Applet Dateizugriff

Einstufung: kritisch
Remote: Ja
Datum: 05.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3640

Die Java-Plattform (englisch Java Platform) definiert die Ablaufumgebung (Java Virtual Machine) und Programmierschnittstellen (Java Application Programming Interface) innerhalb der Java-Technologie. Der Kern der Java-Plattform ist die Java-Laufzeitumgebung (englisch Java Runtime Environment). In verschiedenen Java Paketen wurde eine Schwachstelle identifiziert, durch die mittels eines bösartigen Applets innerhalb von Java Web Start Applikationen beliebige Daten des lokalen gelesen und geschrieben werden können.

Expertenmeinung:
Als populäre Plattform bietet Java ein gerngesehenes Angriffsziel, das auch frequent eingehend untersucht zu werden scheint. Ganze elf Schwachstelle fixt Sun im neusten Update seiner verschiedenen Java-Distributionspakete. In ihrer Kritikalität sind sämtliche Schwachstellen als "kritisch" zu bewerten. Sun hat weiterhin zu einigen Schwachstellen keine Details veröffentlicht, was gemeinhin als tendentiell eher unheilvolles Zeichen zu deuten ist. Nachdem Kompatibilitätsüberprüfungen durchgeführt wurden, sollten Administratoren baldmöglichst die Einspielung aktualisierter Versionen anstreben um die Ausnutzung der hier aufgezeigten Schwachstellen zu vermeiden.

3.11 Sun Java JDK / JRE unspezifizierte Command Execution

Einstufung: kritisch
Remote: Ja
Datum: 05.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3635

Die Java-Plattform (englisch Java Platform) definiert die Ablaufumgebung (Java Virtual Machine) und Programmierschnittstellen (Java Application Programming Interface) innerhalb der Java-Technologie. Der Kern der Java-Plattform ist die Java-Laufzeitumgebung (englisch Java Runtime Environment). In verschiedenen Java Paketen wurde eine Schwachstelle identifiziert, durch die mittels zweier unspezifizierter Fehler beliebige Befehle auf dem Zielsystem ausgeführt werden können.

Expertenmeinung:
Als populäre Plattform bietet Java ein gerngesehenes Angriffsziel, das auch frequent eingehend untersucht zu werden scheint. Ganze elf Schwachstelle fixt Sun im neusten Update seiner verschiedenen Java-Distributionspakete. In ihrer Kritikalität sind sämtliche Schwachstellen als "kritisch" zu bewerten. Sun hat weiterhin zu einigen Schwachstellen keine Details veröffentlicht, was gemeinhin als tendentiell eher unheilvolles Zeichen zu deuten ist. Nachdem Kompatibilitätsüberprüfungen durchgeführt wurden, sollten Administratoren baldmöglichst die Einspielung aktualisierter Versionen anstreben um die Ausnutzung der hier aufgezeigten Schwachstellen zu vermeiden.

3.12 Juniper Networks Secure Access 2000 "delivery_mode" Cross-Site Scripting

Einstufung: problematisch
Remote: Ja
Datum: 04.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3634

Die Firma Juniper Networks, Inc. ist der weltweit zweitgrößte Netzwerkausrüster. Juniper produziert High-End-Router, die im Core- und Edge-Bereich des Internet-Backbone eingesetzt werden. Seit der Gründung im Jahr 1996 verlor Cisco Systems einen nicht unbedeutenden Marktanteil an Juniper Networks. Zwischen 1996 und 2000 stiegen die Anteile von Juniper von 0 % auf 33,5 %, während Cisco in dieser Zeit von 89 % auf 64,7 % abfiel. In dieser Zeit verdiente sich Juniper den Spitznamen „Cisco Killer“. Im Produkt Juniper Networks Secure Access 2000 stellte Richard Brain eine Schwachstelle fest, bei der der Parameter delivery_mode in danana/auth/rdremediate.cgi nicht korrekt verifiziert wird. Daraus resultierend sind beliebige webbasierende Angriffstechniken wie Cross-Site-Scripting oder Cross-Site-Request-Forgery möglich.

Expertenmeinung:
Mit dem stets wachsenden Erfahrungsschatz im Bereich des Web Exploitings werden solche Schwachstellen zunehmend gefährlicher, als sie es so oder so schon sind. Das Problem der Script Injection wird in diesem Kontext nach wie vor zu wenig ernst genommen. Im vorliegenden Fall empfiehlt sich die Einspielung des freigegebenen Patches binnen nützlicher Frist.

3.13 phpMyAdmin "$_REQUEST" SQL Injection

Einstufung: problematisch
Remote: Ja
Datum: 03.03.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3633

phpMyAdmin ist eine freie PHP-Applikation zur Administration von MySQL-Datenbanken. Die Administration erfolgt über HTTP mit einem Browser. Daher können auch Datenbanken auf fremden Rechnern über eine Netzwerkverbindung oder über das Internet administriert werden. Für die Nutzung des Programms sind keine Kenntnisse in SQL notwendig, da die Applikation nach dem WYSIWYG-Verfahren arbeitet. Richard Cunningham meldete dem Hersteller eine Schwachstelle, bei der ein Angreifer sich mittels der $_REQUEST Variable in der Lage sah, beliebige SQL Queries zur Ausführung zu bringen, sofern ein Benutzer eine bösartige Webseite besucht.

Expertenmeinung:
phpMyAdmin gilt heute durchaus als "Standard" für die webbasierte Wartung von MySQL Datenbanken. Zurecht, bietet es doch eine sehr schnelle und einfache Zugriffsmöglichkeit. Im Anbetracht der vorliegenden Schwachstelle empfiehlt es sich, das freigegebene Update baldmöglichst einzuspielen um einen möglichen Angriff zu vermeiden.

3.14 CUPS "process_browse_data()" Double Free Schwachstelle

Einstufung: problematisch
Remote: Teilweise
Datum: 20.02.2008
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3631

Common Unix Printing System (CUPS) ist ein Drucksystem, ein Daemon, der das Drucken unter den verschiedenen Unix-artigen Betriebssystemen ermöglicht. CUPS wurde vom Unternehmen Easy Software Products entwickelt und kann sowohl unter der GPL als auch unter proprietären Lizenzen verwendet werden. Es wurde als Nachfolger von älteren Drucksystemen, wie beispielsweise LPD, entworfen. H. Blitschke entdeckte eine Schwachstelle, bei der durch ein manipuliertes Paket an den Port tcp/631 einen Denial of Service verursacht werden kann.

Expertenmeinung:
CUPS ist heute ein Standardprotokoll im Linuxumfeld und entsprechend angreifbar. Der freigegebene Patch für entsprechende Implementierungen sollte zeitnah eingespielt werden, um die Ausnutzung zu vermeiden.

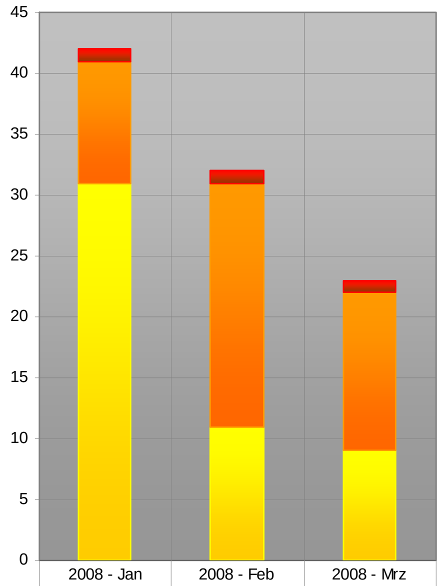
4. Statistiken Verletzbarkeiten

Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeits-datenbank der scip AG.

http://www.scip.ch/cgi-bin/smss/showadvf.pl

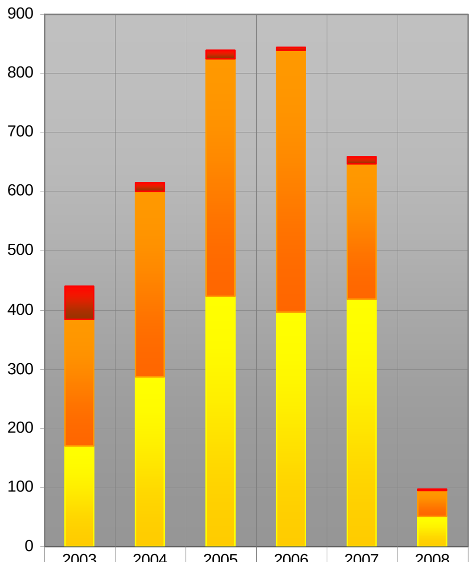
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbar-keitsdatenbank wünschen so senden Sie uns eine E-Mail an mailto:info@scip.ch. Gerne neh-men wir Ihre Vorschläge entgegen.

Auswertungsdatum:	19. März 2008



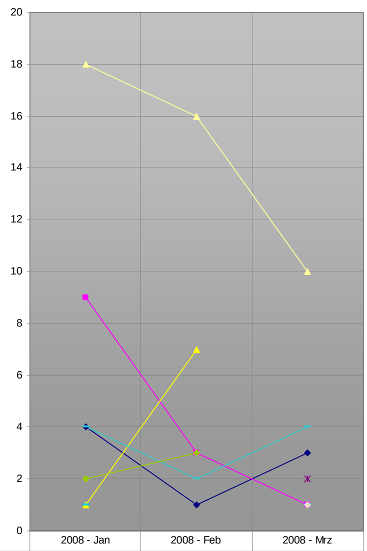
	2008 - Jan	2008 - Feb	2008 - Mrz
sehr kritisch	1	1	1
kritisch	10	20	13
problematisch	31	11	9

Verlauf der Anzahl Schwachstellen pro Jahr



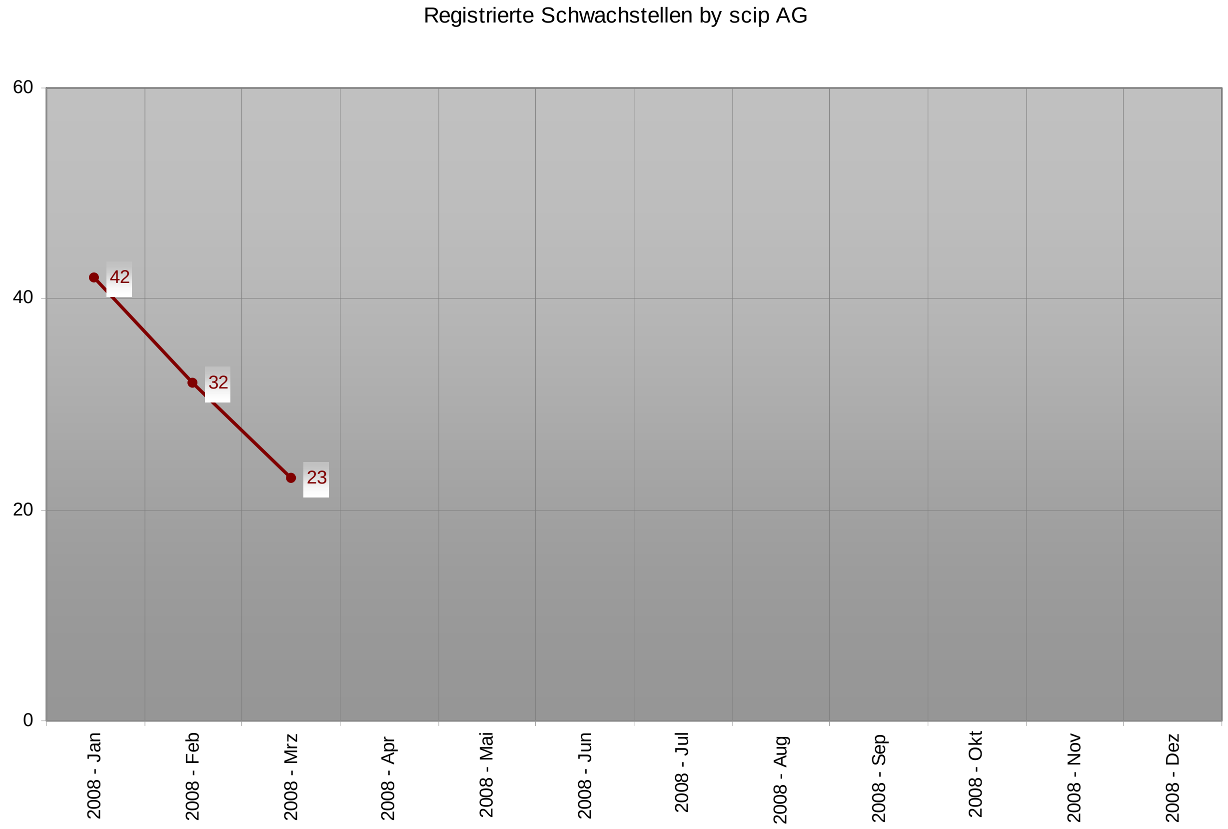
	2003	2004	2005	2006	2007	2008
sehr kritisch	56	15	15	6	11	3
kritisch	214	314	402	442	229	43
problematisch	170	287	423	396	419	51

Verlauf der letzten drei Monate Schwachstelle/Schweregrad

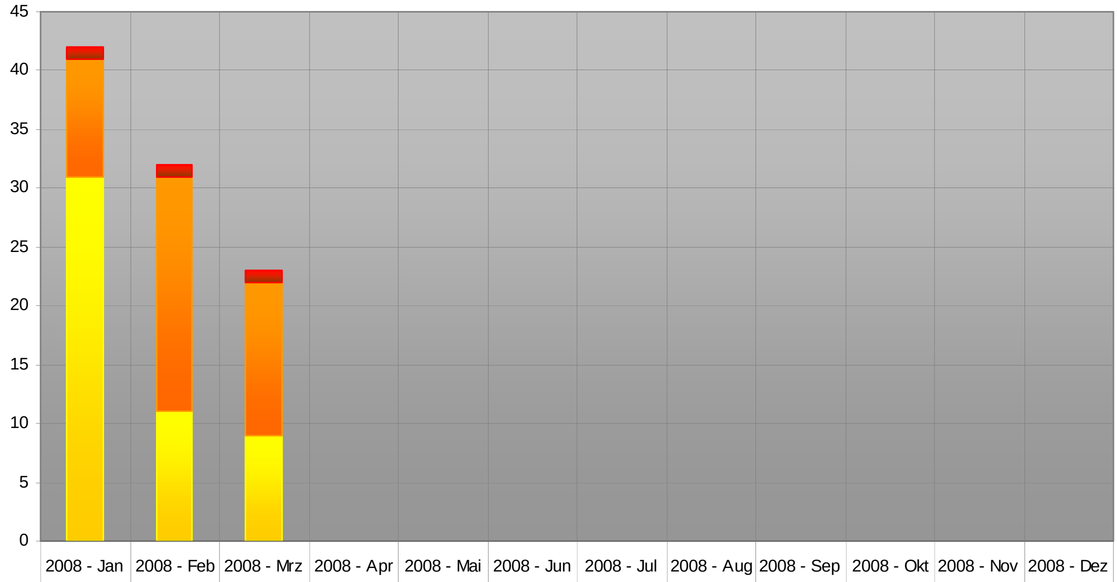


	2008 - Jan	2008 - Feb	2008 - Mrz
Cross Site Scripting (XSS)	4	1	3
Denial of Service (DoS)	9	3	1
Designfehler	1	7	
Directory Traversal			
Eingabeungültigkeit			2
Fehlende Authentifizierung			
Fehlende Verschlüsselung			
Fehlerhafte Leserechte	1		
Fehlerhafte Schreibrechte	1		1
Format String			1
Konfigurationsfehler			
Pufferüberlauf	18	16	10
Race-Condition			
Schwache Authentifizierung			
Schwache Verschlüsselung			
SQL-Injection	2		1
Symlink-Schwachstelle			
Umgehungs-Angriff	4	2	4
Unbekannt	2	3	

Verlauf der letzten drei Monate Schwachstelle/Kategorie

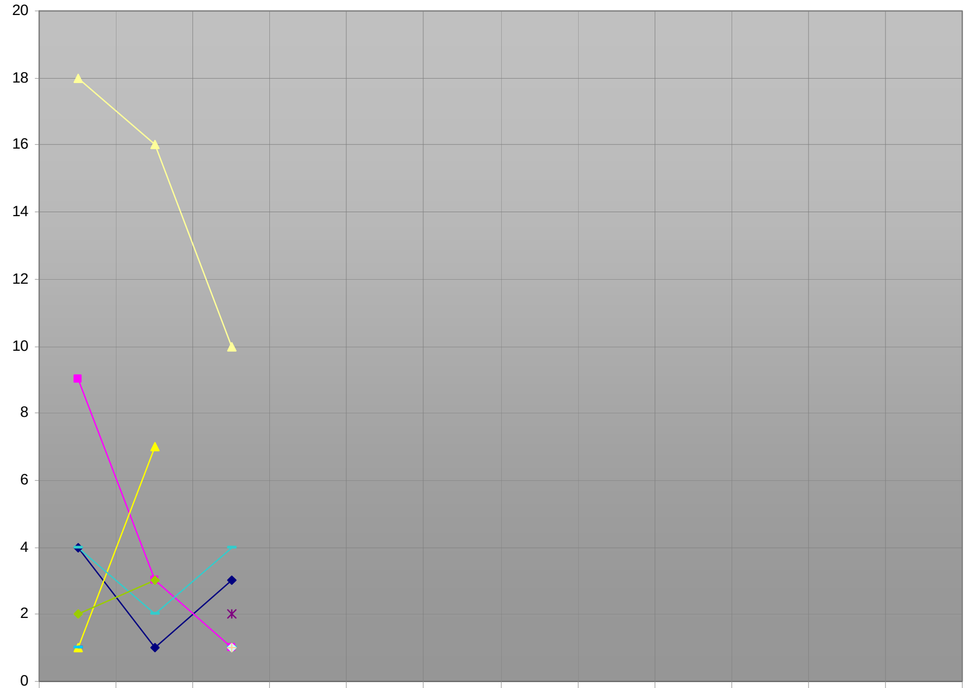


Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008



	2008 - Jan	2008 - Feb	2008 - Mrz	2008 - Apr	2008 - Mai	2008 - Jun	2008 - Jul	2008 - Aug	2008 - Sep	2008 - Okt	2008 - Nov	2008 - Dez
sehr kritisch	1	1	1									
kritisch	10	20	13									
problematisch	31	11	9									

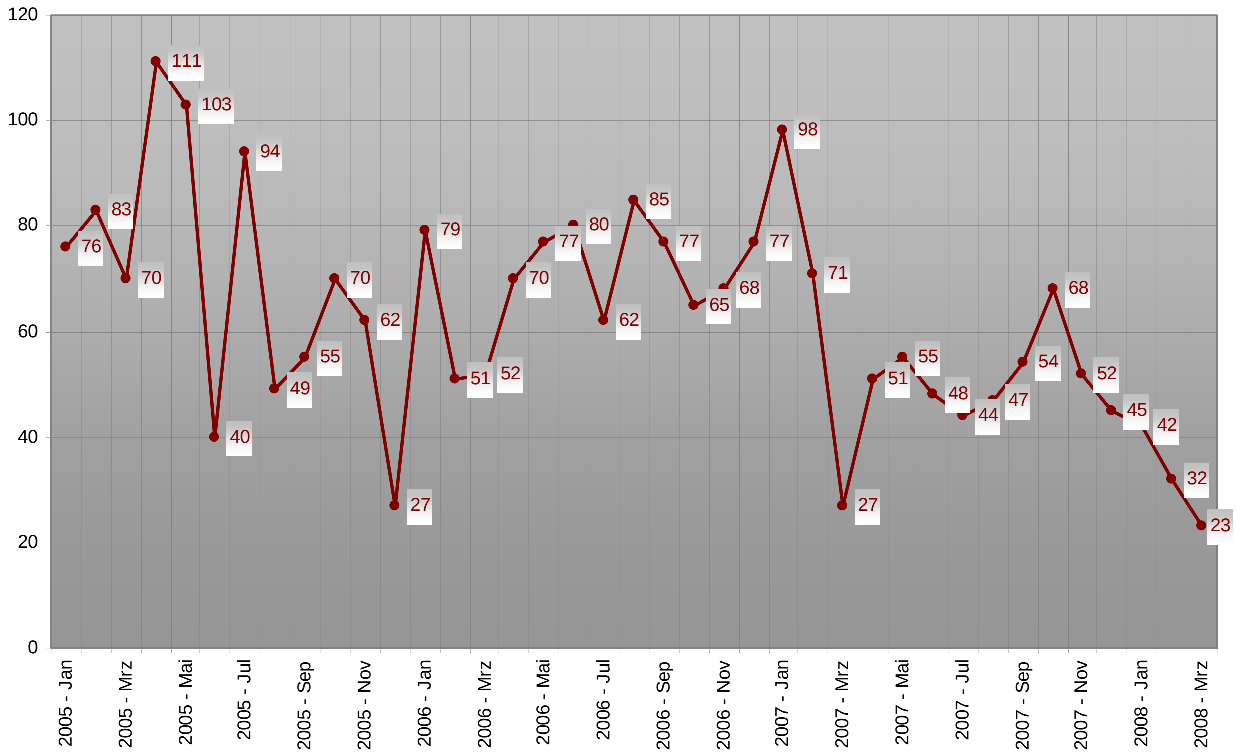
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2008



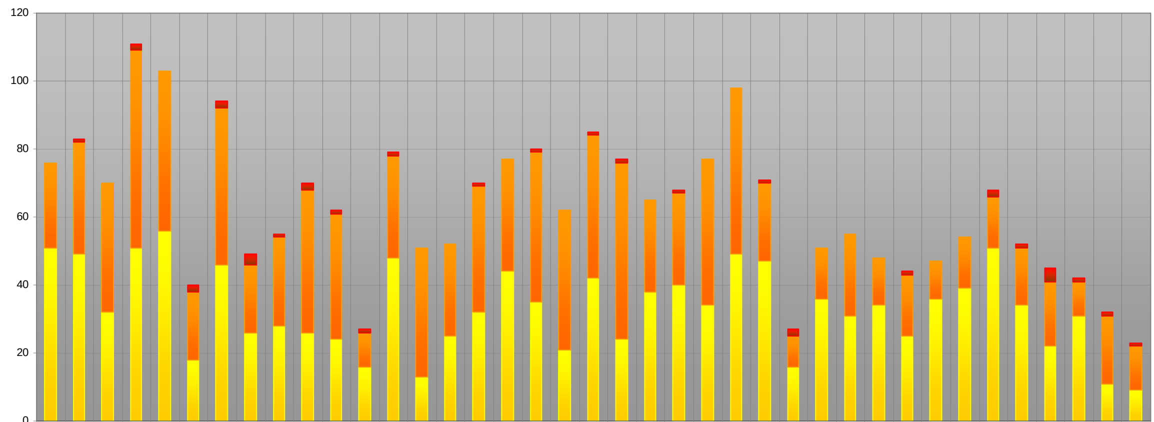
	2008 - Jan	2008 - Feb	2008 - Mrz	2008 - Apr	2008 - Mai	2008 - Jun	2008 - Jul	2008 - Aug	2008 - Sep	2008 - Okt	2008 - Nov	2008 - Dez
Cross Site Scripting (XSS)	4	1	3									
Denial of Service (DoS)	9	3	1									
Designfehler	1	7										
Directory Traversal												
Eingabeungültigkeit			2									
Fehlende Authentifizierung												
Fehlende Verschlüsselung												
Fehlerhafte Leserechte	1											
Fehlerhafte Schreibrechte	1		1									
Format String			1									
Konfigurationsfehler												
Pufferüberlauf	18	16	10									
Race-Condition												
Schwache Authentifizierung												
Schwache Verschlüsselung												
SQL-Injection	2		1									
Symlink-Schwachstelle												
Umgehungs-Angriff	4	2	4									

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2008

Registrierte Schwachstellen by scip AG



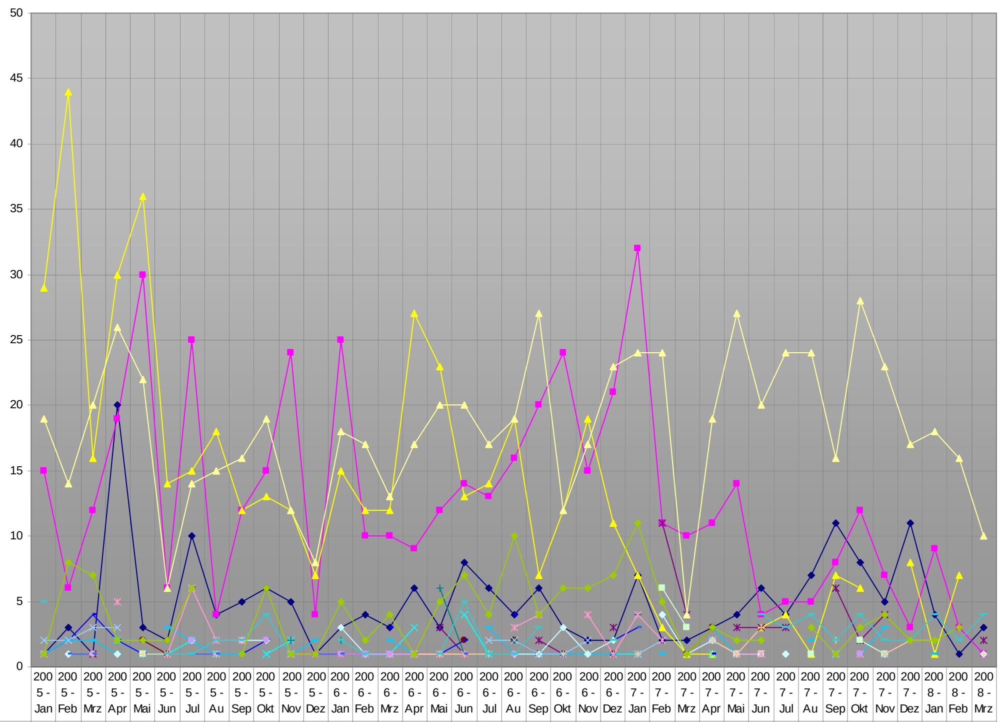
Verlauf der Anzahl Schwachstellen pro Monat seit Januar2005



	2005 - Jan	2005 - Feb	2005 - Mrz	2005 - Apr	2005 - Mai	2005 - Jun	2005 - Jul	2005 - Aug	2005 - Sep	2005 - Okt	2005 - Nov	2005 - Dez	2006 - Jan	2006 - Feb	2006 - Mrz	2006 - Apr	2006 - Mai	2006 - Jun	2006 - Jul
sehr kritisch		1		2		2	2	3	1	2	1	1	1			1		1	
kritisch	25	33	38	58	47	20	46	20	26	42	37	10	30	38	27	37	33	44	41
problematisch	51	49	32	51	56	18	46	26	28	26	24	16	48	13	25	32	44	35	21

	2006 - Aug	2006 - Sep	2006 - Okt	2006 - Nov	2006 - Dez	2007 - Jan	2007 - Feb	2007 - Mrz	2007 - Apr	2007 - Mai	2007 - Jun	2007 - Jul	2007 - Aug	2007 - Sep	2007 - Okt	2007 - Nov	2007 - Dez	2008 - Jan	2008 - Feb	2008 - Mrz
sehr kritisch	1	1		1			1	2				1			2	1	4	1	1	1
kritisch	42	52	27	27	43	49	23	9	15	24	14	18	11	15	15	17	19	10	20	13
problematisch	42	24	38	40	34	49	47	16	36	31	34	25	36	39	51	34	22	31	11	9

Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat seit Januar 2005



	2005-Jan	2005-Feb	2005-Mrz	2005-Apr	2005-Mai	2005-Jun	2005-Jul	2005-Au	2005-Sep	2005-Okt	2005-Nov	2005-Dez	2006-Jan	2006-Feb	2006-Mrz	2006-Apr	2006-Mai	2006-Jun	2006-Jul	2006-Au	2006-Sep	2006-Okt	2006-Nov	2006-Dez	2007-Jan	2007-Feb	2007-Mrz	2007-Apr	2007-Mai	2007-Jun	2007-Jul	2007-Au	2007-Sep	2007-Okt	2007-Nov	2007-Dez	2008-Jan	2008-Feb	2008-Mrz
Cross Site Scripting (XSS)	1	3	1	20	3	2	10	4	5	6	5	1	3	4	3	6	3	8	6	4	6	3	2	2	7	2	2	3	4	6	4	7	11	8	5	11	4	1	3
Denial of Service (DoS)	15	6	12	19	30	6	25	4	12	15	24	4	25	10	10	9	12	14	13	16	20	24	15	21	32	11	10	11	14	4	5	5	8	12	7	3	9	3	1
Designfehler	29	44	16	30	36	14	15	18	12	13	12	7	15	12	12	27	23	13	14	19	7	12	19	11	7	3	1	1		3	4	1	7	6		8	1	7	
Directory Traversal				2	1	1	2			1	2			1	1	3		4	1					1	1			1											
Eingabeungültigkeit			1			1						1	1	1			3	1			2	1		3		11	4		3	3	3		6	2	4				2
Fehlende Authentifizierung			1		2	1							1					2		2	1	1		1			1	3											
Fehlende Verschlüsselung					2		2		1		2		2		1		6	1		2			1		4														
Fehlerhafte Leserechte	1	2	4	2	1		6		1	2			1		3		1	2		4				2	3			1									1		
Fehlerhafte Schreibrechte	1	2	2	1		3	2	1	1		1	2			2	1			3	1	1	1	1	1		1		3	1			2		1	3		1		1
Format String		1		1			2		2	2			3	1	1	1				1	1	3	1	2		4	1	2			1				1				1
Konfigurationsfehler					1																					6	3		1	1		1		2	1				
Pufferüberlauf	19	14	20	26	22	6	14	15	16	19	12	8	18	17	13	17	20	20	17	19	27	12	17	23	24	24	4	19	27	20	24	24	16	28	23	17	18	16	10
Race-Condition	2	2	3	3		1		1			1			1		1	1		2	2	1	1	2		1	2		2	1	1			1		1				
Schwache Authentifizierung	1			5		1	6	2	2		1	1	1		1	1	1	1		3	4		4	1	4	2			1	1				1					
Schwache Verschlüsselung	1		1				2			2			1	1	1	1				1														1					
SQL-Injection			1		1	1		1				1				1	1	1	1			1			1			2	1	3			2		1	2	2		1
Symlink-Schwachstelle		1	1		2		1	1				1	1			1		1							3														
Umgehungs-Angriff	5					1	1	2	2	4	1		2	1			1	5	1	1	3			2						4	3	4	2	4	2	2	4	2	4
Unbekannt	1	8	7	2	2	2	6		1	6	1	1	5	2	4	1	5	7	4	10	4	6	6	7	11	5	1	3	2	2		3	1	3	4	2	2	3	

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat seit Januar 2005

5. Bilderrätsel

GESUCHTE BEGRIFFE

5 Buchstaben (engl.)	8 Buchstaben (engl.)	7 Buchstaben

LÖSUNGSWORT

Wettbewerb

Mailen Sie uns das erarbeitete Lösungswort an die Adresse mailto:info@scip.ch inklusive Ihren Kontakt-Koordinaten. Das Los entscheidet über die Vergabe des Preises. Teilnahmeberechtigt sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.04.2008**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung des Bilderrätsel finden Sie jeweils online auf http://www.scip.ch unter Publikationen > scip monthly Security Summary > Errata.

Gewinnen Sie einen Monat des Securitytracker Dienstes)pallas(.

6. Impressum

Herausgeber:

scip AG
Badenerstrasse 551
CH-8048 Zürich
T +41 44 404 13 13
mailto:info@scip.ch
http://www.scip.ch

Zuständige Person:

Marc Ruef
Security Consultant
T +41 44 404 13 13
mailto:maru@scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserungen möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summarys finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. Anmelden! Abmelden!